DATA BREACHES COST COMPANIES MILLIONS PER YEAR, GLOBALLY
Little Being Done To Prevent Data Theft In Major Companies. Is Your Data Safe?

Data Breaches Defined

Stories about customer's private data being compromised are becoming so commonplace that most people are not surprised anymore. They are termed "data breaches" but what exactly does that mean?

A data breach is when a person's identifying information, along with a record of some kind from an institution is either stolen (the most common cause), or accidentally released to unauthorized parties.

These records can include a person's name, address, tax information, credit card numbers, or medical history—and the list goes on. Most breaches contain 10,000 or fewer records, with breaches in the 100,000 record range the minority.

There are three ways a data breach can happen: intentional theft or system compromise, a technical system error, or by a human-caused accidental leak.

How Common Are They?

According to a recent study by Ponemon Institute that was commissioned by IBM, "...the likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 22 percent over a 24-month period, the chances of a data breach involving a 100,000 records is less than 1 percent..." The study queried 314 companies in 16 industries, in 10 countries.

Numbers provided by the study show that the USA tops the list of the average number of breached records with 29,087, followed by the Arabian region with 28,690, and India with 26,586.

Cost of Data Breaches

The report found that "German and US companies had the most costly data breaches ($195 and $201 per record, respectively). These countries also experienced the highest total cost (US at $5.85 million and Germany at $4.74 million)." Costs include lost business and mitigation of future breaches. The top industries affected costs-wise are: healthcare, education, and pharmaceuticals.

One of the largest costs in a data breach is the post-breach cost, which is over $1.5 million USD on average. Actions taken include notification of the people affected, help desk fees, investigative analysis, legal expenses, and regulatory compliance.

32 percent of companies included in the study are now purchasing "cyber insurance" at an added annual cost.

Prevention

Defense against data breaches is no easy matter. Instituting hardened IT security systems and protocols, such as mobile device management (a major source of data breaches), are the most effective deterrents. Amazingly, the findings show that "...strategies to protect online presence, information assets and infrastructure do not exist for most of the companies represented in this research."

Data breaches show no sign of slowing and are likely to only increase, especially when the companies involved lack the tools to minimize them.

Read the Complete Report

Click here to download the free PDF.